SERVIZIO BOOLEANO DI VERIFICA CORRISPONDENZA FRA SOGGETTO GIURIDICO E SUO RAPPRESENTANTE LEGALE

SPECIFICHE TECNICHE

Indice

.

1. GENERALITÀ DEL SERVIZIO

Il presente documento descrive le modalità di utilizzo del servizio web-services per la verifica di corrispondenza fra il codice fiscale del rappresentante legale di un soggetto giuridico e il soggetto giuridico stesso. L'esito della verifica è un valore booleano restituito. Il riscontro viene effettuato sull'Archivio Anagrafico dell'Agenzia delle Entrate, secondo i seguenti criteri concordati:

- a partire da una coppia di codici fiscali appartenenti a Rappresentante e Ente rappresentato, il servizio fornisce un esito booleano di effettiva associazione Rappresentante/Rappresentato.
- la verifica dovrà riferirsi alla situazione in Anagrafe Tributaria al momento del richiamo del servizio e verrà eseguita sia per il Rappresentante principale dell'Ente (Quadro C modd. AA7 o AA5), sia per gli altri Rappresentanti (Quadro F mod. AA7 con selezione della casella "R").
- il codice fiscale Ente potrà corrispondere esclusivamente a soggetto diverso dalle persone fisiche, con o senza partita IVA.
- i codici fiscali dell'Ente e del Rappresentante sono stati validati prima dell'accesso al servizio.

Il servizio è disponibile nei due ambienti paralleli:

- **Ambiente di TEST/SPERIMENTAZIONE:** l'ambiente viene utilizzato sia in fase di prima attivazione per emulare le verifiche agganciando la base dati anagrafica di test, sia in sperimentazione come ambiente di riferimento per le attività di manutenzione o implementazione.
  La url con cui richiamare il servizio in ambiente di validazione sarà fornita non appena il servizio sarà configurato nei sistemi dell'Anagrafe Tributaria

- **Ambiente di GESTIONE**, utilizzato a regime per il riscontro dei soggetti sull' Archivio Anagrafico dell'Anagrafe Tributaria.
  Il servizio è richiamabile con la seguente url:
  La url con cui richiamare il servizio in ambiente di produzione sarà fornita non appena il servizio sarà configurato nei sistemi dell'Anagrafe Tributaria

In allegato al documento sono riportati:

Allegato 1 - Specifiche Tecniche delle strutture dati in Richiesta e Risposta: All1_specifiche tecniche_tracciati.pdf

Allegato 2 – Specifiche di Accesso in Sicurezza: All2_Specifiche di accesso in sicurezza.pdf

Allegato 3 – Wsdl ed xsd del servizio: All3_WSDL_allegati_v1.0.zip

2. MODALITA' DI UTILIZZO DEL SERVIZIO

Nell' allegato 1) è riportata la specifica tecnica in formato tabellare che dettaglia il contenuto informativo del servizio, il formato dei campi forniti e gli eventuali valori ammessi, i controlli effettuati sui campi forniti in richiesta e i codici di errore impostati di conseguenza.

A seguito del Provvedimento emesso dall' Autorità Garante il 18 settembre 2008 per la protezione dei dati personali (e successive integrazioni di marzo 2010 - sezione "Specifiche tecniche della nuova classe di web-services") inerente l'erogazione di web-services da parte dell'Agenzia Entrate, è stata predisposta una infrastruttura di erogazione dei servizi integrata di una "Cornice di sicurezza", per ottemperare alle misure previste.

L'infrastruttura predisposta consente di utilizzare il servizio con accesso da rete Internet, all'interno di un sistema di Identità Federata, nel quale l'Agenzia Entrate rappresenta il fornitore del servizio (Service Provider SP) mentre l'Ente fruitore del servizio stesso, assume il ruolo di fornitore di identità (Identity Provider IdP).

L'Ente che intende partecipare all'Identità Federata, dovrà sottoscrivere un accordo di trust, nel quale saranno specificate le politiche di sicurezza che l'Ente si impegna a rispettare al proprio interno (ad esempio le password policy applicate dall'Ente nel proprio sistema per le credenziali degli utenti).
Gli utenti dell'Ente Identity Provider, potranno accedere ai servizi esposti dall'Agenzia mediante l'utilizzo di applicazioni dell'Ente stesso, autenticandosi presso il proprio sistema con le credenziali da questo rilasciate.

2.1. Cornice di Sicurezza

Con il termine "cornice di sicurezza" si intende una particolare configurazione che prevede l'utilizzo di protocolli di Identità Federata (SAML) per uniformarsi alle direttive del Garante per la Privacy, in materia di cooperazione applicativa mediante utilizzo dei web services.

L'utente si autentica sul proprio Identity Provider che rilascia una asserzione SAML. Tale asserzione viene inserita nel WS-Security Header della SOAPRequest inviata al sistema dell'Agenzia Entrate, come riscontro dell'avvenuta autenticazione.

L'asserzione SAML contiene come utenza l'identificativo dell'Ente Identity Provider, mentre il reale user o identificativo dell'utente autenticato e altre informazioni utili per il tracciamento degli accessi, sono contenute negli attributi dell'asserzione stessa.

In tale contesto, la fruizione dei servizi si basa sui protocolli previsti dallo standard WS-Security (Web Service Security), strutturato nei diversi componenti:

1) Fase di autenticazione/autorizzazione, mediante l'utilizzo dello standard di federazione SAML; l'utente dell'Ente si autentica sul proprio sistema che rilascia, per lo stesso, una asserzione SAML.
   Tale asserzione, che viene firmata dall'Ente, viene inserita nel WS-Security Header della SOAPRequest inviata ai server dell'Agenzia a testimonianza dell'avvenuta autenticazione.
   L'asserzione SAML , che come utenza (NameId) deve assumere il seguente valore **cffruitore/XXX** (anche questo dato sarà fornito prima dell'attivazione del servizio), è inoltre strutturata con i seguenti attributi:
   - Un attributo contenente il reale userid o codice fiscale dell'utente (User)
   - Un attributo contenente l'IP della postazione client assegnata nell'ambito dell'Ente all'utente (IP-User).

2) Fase di accertamento della firma attraverso la quale il sistema dell'Agenzia Entrate verifica la validità dell'asserzione contenuta nel WS-Security Header della SOAPRequest.

3) Fase di inoltro della richiesta SOAP, per cui l'infrastruttura rimanda la richiesta al sistema interno per l'elaborazione, corredandola con opportuni token e attributi custom per consentire la gestione delle ulteriori verifiche di profilazione e le attività di tracciamento delle operazioni.

   Per un maggior dettaglio relativamente all'accesso in sicurezza, si rimanda all'allegato 2).

2.2. Tracciamento delle operazioni

L'Autorità Garante, sempre nel provvedimento marzo 2010, precisa che il sistema di tracciamento dell'Ente Service Provider, oltre a registrare le informazioni rese disponibili dal servizio erogato, acquisisca anche le informazioni ricevute mediante l'asserzione SAML.

Pertanto, per ottemperare alle prescrizioni del Garante, sono stati integrati nel tracciamento degli accessi effettuati mediante utilizzo dei Web Services, i seguenti dati:

Ente connesso, desunto dal NameId presente nell'asserzione SAML
Utente remoto dell'Ente (User), desunto dall'attributo dell'asserzione SAML
Indirizzo IP della postazione dell'utente connesso, desunta dall'attributo dell'asserzione SAML (IP-User).